

**UNITED STATES DISTRICT COURT FOR THE
NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION**

CAMERON KING, individually, and on
behalf of himself and all similarly situated
persons,

Plaintiff,

v.

AT&T, INC.,

Defendant.

Case No. 3:24-cv-00867

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Cameron King (the "Plaintiff"), both individually and as a representative of all others similarly situated, initiates this legal action against Defendant AT&T, Inc. ("AT&T"), a Texas corporation, seeking damages, restitution, and injunctive relief for the Class, as defined below. Plaintiff asserts the following allegations based on information and belief, with the exception of his own actions, the investigation conducted by his counsel, and facts that are a matter of public record.

NATURE OF THE ACTION

1. This class action stems from a recent deliberate cyberattack and data breach (the "Data Breach"), where AT&T, the largest telecommunications services company in the United States, experienced a loss of control over the personal data and sensitive information of over 73 million current and former customers. AT&T estimates that approximately 7.6 million current account holders and 65.4 million former account holders have been impacted.¹ These affected customers, which include Plaintiffs and Class Members, experienced identifiable damages due to this breach, such

¹ <https://www.npr.org/2024/03/30/1241863710/att-data-breach-dark-web>.

as loss of expected benefits, incurred expenses, and the and the time expended to address or mitigate the consequences of the attack.

2. The personal data and sensitive information of both the Plaintiff and Class Members, which were entrusted to AT&T for safekeeping, were compromised and unlawfully accessed as a result of the Data Breach.

3. The Data Breach encompassed personally identifiable information ("PII") that the AT&T collected and maintained. Information compromised in the Data Breach includes, among other things, names, addresses, phone numbers, dates of birth, Social Security Numbers, and email addresses ("Private Information").

4. Plaintiff initiates this class action lawsuit to redress AT&T's insufficient safeguarding of Class Members' Private Information that it collected, as well as its failure to promptly and adequately notify Plaintiff and Class Members about the unauthorized access of their information by unknown third parties, including the precise nature of the information accessed.

5. AT&T, in a recklessness manner, not only collected but also shared Private Information without due diligence or regard for privacy safeguards. This reckless behavior, which transgresses the norms of responsible data handling, poses significant risks to the confidentiality and security of individuals' sensitive information. By neglecting to implement adequate measures to safeguard Private Information and heedlessly sharing it, AT&T has shown a blatant disregard for the privacy rights and security concerns of those whose information it was entrusted with. Such irresponsible actions not only undermine trust but also expose individuals to potential exploitation and harm from malicious actors seeking to exploit vulnerabilities in data security protocols.

6. As custodians of sensitive information, corporations like the AT&T have a paramount responsibility to exercise prudence and diligence in handling Private Information to prevent

unauthorized access and ensure the protection of individuals' privacy rights. Therefore, AT&T's reckless collection and dissemination of Private Information warrant thorough scrutiny and appropriate accountability measures to rectify the harm caused and prevent future breaches of trust.

7. Specifically, AT&T not only gathered Private Information but also neglected to enact sufficient security measures to protect it. Additionally, the company opted to retain the Private Information of former customers, needlessly exposing them to risk. Furthermore, this sensitive data was shared with a vendor lacking sufficient cybersecurity protections, thereby exacerbating the risk of unauthorized access and misuse. This negligent handling of Private Information by AT&T not only highlights a breach of trust but also underscores a concerning lack of diligence in ensuring the protection of individuals' privacy. By entrusting sensitive data to a vendor with insufficient cybersecurity safeguards, AT&T further compounded the vulnerability of this information, leaving it susceptible to exploitation by malicious actors. Such practices not only jeopardize the confidentiality and integrity of Private Information but also demonstrate a disregard for the importance of robust data security protocols. It is imperative for organizations to recognize the gravity of their responsibility in safeguarding Private Information and to take proactive measures to mitigate risks and protect individuals' privacy rights.

8. Therefore, AT&T's actions in collecting, inadequately securing, and sharing Private Information with a vulnerable vendor warrant comprehensive review and remedial action to address the potential harm inflicted and prevent similar lapses in the future.

9. Upon information and belief, AT&T was aware of the cyberattack risks and potential for disclosing Private Information belonging to the Plaintiff and Class Members. Failing to address these risks left the information vulnerable. This neglect demonstrates a disregard for data security and

the safety of individuals' sensitive data. Hence, corrective action is imperative to prevent further harm and protect privacy rights.

10. As a result, the negligent conduct of AT&T has heightened the risk of identity theft for both the Plaintiff and Class Members. The Private Information entrusted to AT&T, which it pledged to safeguard, is now in the possession of data thieves, further jeopardizing the security of individuals' identities.

11. Equipped with the Private Information obtained through the Data Breach, cybercriminals have the ability to perpetrate numerous crimes. These may include, for instance, opening new financial accounts, securing loans, accessing government benefits, filing fraudulent tax returns, obtaining driver's licenses using a Class Member's name but with another individual's photograph, and providing false information to law enforcement during an arrest.

12. Due to the Data Breach, both the Plaintiff and Class Members face an elevated and immediate threat of fraud and identity theft. Consequently, they are compelled to diligently monitor their financial accounts both presently and in the future to safeguard against potential identity theft.

13. The Plaintiff and Class Members may additionally bear expenses such as purchasing credit monitoring services, implementing credit freezes, obtaining credit reports, or investing in other protective measures aimed at preventing and identifying instances of identity theft.

14. The Plaintiff seeks to address these damages on behalf of himself and all others similarly affected, whose Private Information was compromised during the Data Breach.

15. The Plaintiff is seeking remedies that encompass, among other possibilities, compensatory damages, reimbursement for incurred expenses, and injunctive relief. This includes enhancements to AT&T's data security protocols, annual audits in the future, and provision of adequate credit monitoring services funded by AT&T.

PARTIES

16. Plaintiff Cameron King, a citizen of California, has been an AT&T customer since 2006, continuously receiving telecommunication services from the company.

17. Defendant AT&T is a telecommunications company offering an array of services, including wireless network services, cellular data plans, cell phone packages, and Internet connectivity plans, among other offerings.

18. AT&T is headquartered and has its principal place of business at 208 South Akard Street Dallas, Texas 75202, and may be served via their registered agent CT Corporation System, 1999 Bryan Street., Ste. 900, Dallas, Texas 75201. Defendant is a citizen of Texas.

JURISDICTION AND VENUE

19. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds \$5 million, exclusive of interest and costs. Upon information and belief, the number of class members is over 100, many of whom have different citizenship from AT&T. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

20. This Court has personal jurisdiction over AT&T because AT&T is headquartered and has its principal place of business in the Dallas Division of the Northern District of Texas and has thus availed itself of the rights and benefits of the State of Texas by, *inter alia*, engaging in activities including (i) directly and/or through its parent companies, affiliates and/or agents providing services throughout the United States in this judicial district and abroad; (ii) conducting substantial business in this forum; (iii) having a registered agent to accept service of process in the State of Texas; and/or (iv) engaging in other persistent courses of conduct and/or deriving substantial revenue from services provided in Texas and in this judicial District.

21. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in the Dallas Division of the Northern District of Texas.

AT&T'S BUSINESS

22. AT&T is a company that provides telecommunications services across the United States.

23. In the course of providing telecommunications services, AT&T requires customers to provide certain Private Information. This includes various types of personal data outlined in its Privacy Notice:

- **Account Information:** You give us information about yourself, such as contact and billing information. We also keep service-related history and details, including Customer Proprietary Network Information.
- **Equipment Information:** We collect information about equipment on our network like the type of device you use, device ID, and phone number.
- **Network Performance:** We monitor and test the health and performance of our network. This includes your use of Products and Services to show how our network and your device are working.
- **Location Information:** Location data is automatically generated when devices, products and services interact with cell towers and Wi-Fi routers. Location can also be generated by Bluetooth services, network devices and other tech, including GPS satellites.
- **Web Browsing and App Information:** We automatically collect a variety of information which may include time spent on websites or apps, website and IP

addresses and advertising IDs. It also can include links and ads seen, videos watched, search terms entered and items placed in online AT&T shopping carts. We may use pixels, cookies and similar tools to collect this information. We don't decrypt information from secure websites or apps – such as passwords or banking information.

- **Biometric Information:** Fingerprints, voice prints and face scans are examples of biological characteristics that may be used to identify individuals. Learn more in our Biometric Information Privacy Notice.
- **Third-Party Information:** We get information from outside sources like credit reports, marketing mailing lists and commercially available demographic and geographic data. Social media posts also may be collected, if you reach out to us directly or mention AT&T.

24. All such information above is considered Personal Information if it can reasonably link back to identifiable individuals or households. This includes data tied to names, account numbers, or devices.²

25. In its Privacy Notice, AT&T asserts its commitment to maintaining the privacy and security of Private Information with the following statements:

- Thank you for reading our Privacy Notice. *Your privacy is important to you and to us.*

...

- This notice applies to AT&T products and services including internet, wireless, voice and AT&T apps.

² *AT&T Privacy Notice*, AT&T, Inc., <https://about.att.com/privacy/privacy-notice.html> (last accessed April 9, 2024).

...

- **Your privacy choices and controls**

You can manage how we use and share your information for certain activities including advertising and marketing. Here are key examples:

- **Do not sell or share my personal information.** We may share information with other companies in limited ways, such as exchanging subscriber lists for joint marketing.

...

- **Data retention and security**

We work hard to safeguard your information using technology controls and organizational controls. We protect our computer storage and network equipment. We require employees to authenticate themselves to access sensitive data. We limit access to personal information to the people who need access for their jobs. And we require callers and online users to authenticate themselves before we provide account information.

*No security measures are perfect. We can't guarantee that your information will never be disclosed in a manner inconsistent with this notice. If a breach occurs, we'll notify you as required by law.*³

26. Given the highly sensitive and personal nature of the information it handles, AT&T pledges in its Privacy Notice to uphold the confidentiality and security of Private Information, among other commitments.

27. As a prerequisite for accessing its telecommunications services, AT&T mandates that

³ *Id.* (Emphasis added).

its customers entrust it with highly sensitive personal information.

28. In acquiring, collecting, utilizing, and benefiting from the Private Information of the Plaintiff and Class Members, AT&T undertook legal and equitable obligations. It was aware or should have been aware of its responsibility to safeguard the Private Information of the Plaintiff and Class Members from unauthorized disclosure.

29. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

30. Plaintiff and the Class Members trusted AT&T to maintain the confidentiality and security of their Private Information, to solely utilize this data for business purposes, and to make authorized disclosures only.

THE DATA BREACH

A. 2021 Data Incident

31. On or about August 19, 2021, a criminal hacking group called “ShinyHunters” began selling on a hacking forum a database which, according to ShinyHunters, contains Personal Customer Data of over 70 million AT&T customers (the “2021 Data Incident”)⁴

32. While attempting to sell the database, ShinyHunters only revealed sample data from the compromised database, which included customers’ names, addresses, phone numbers, Social Security numbers, and dates of birth.⁵

33. AT&T asserted, without substantiating evidence, that the leaked data samples originated from sources outside of its systems and denied any breach of its own infrastructure.⁶

⁴ *AT&T denies data breach after hacker auctions 70 million user database*, BleepingComputer (Aug. 20, 2021), <https://www.bleepingcomputer.com/news/security/atandt-denies-data-breach-after-hacker-auctions-70-million-user-database/>.

⁵ *Id.*

⁶ *Id.*

34. AT&T also refrained from confirming whether the leaked data stemmed from a breach of a third-party partner's information technology systems, which potentially housed sensitive Private Information.⁷

35. ShinyHunters contested AT&T's denials regarding the origin of the Data Breach, whether from AT&T or one of its third-party partners, asserting, "I don't care if they don't admit it. I'm simply selling."⁸

36. ShinyHunters additionally mentioned that the criminal group was open to "negotiating" with AT&T.⁹

37. Shortly following the 2021 Data Incident, a security researcher reported that among the data samples leaked by ShinyHunters, two out of the four individuals were verified to possess accounts on att.com.¹⁰

38. Notwithstanding, AT&T chose not to notify any of its customers, including Plaintiff and Class Members, of the 2021 Data Incident.

B. 2024 Data Incident

39. On or around March 17, 2024, a cybercriminal referred to as "MajorNelson" uploaded the complete dataset from the 2021 Data Incident, which ShinyHunters had previously attempted to sell, onto an internet forum.¹¹

40. The data disclosed by MajorNelson comprised various data types from approximately

⁷ *Id.*

⁸ *Id.*

⁹ *Id.*

¹⁰ *Id.*

¹¹ *AT&T says leaked data of 70 million people is not from its systems*, BleepingComputer (Mar. 17, 2024), <https://www.bleepingcomputer.com/news/security/att-says-leaked-data-of-70-million-people-is-not-from-its-systems/amp/> (last visited on Apr. 9, 2024).

7.6 million current account holders and 65.4 million former account holders,¹² including but not limited to: names, addresses, phone numbers, dates of birth, and Social Security numbers.¹³

41. On March 19, 2024, Troy Hunt, a renowned security researcher and the creator of the data breach notification website "Have I Been Pwned," addressed the AT&T Data Breach in a blog post.¹⁴

42. In his blog post, Mr. Hunt reached the conclusion that the leaked data from the Data Breach was indeed authentic. He arrived at this determination after conversing with numerous "Have I Been Pwned" subscribers who were AT&T customers and verified the accuracy of the leaked data.¹⁵

43. Further, Mr. Hunt observed that the Internet forum where the leaked data was posted is not situated on the 'dark web' but rather on the conventional web, accessible "easily by a standard web browser."¹⁶

44. The combination of the 2021 Data Incident with the 2024 Data Incident (the "Data Breach") resulted in substantial harm to the Plaintiff and Class Members.

C. AT&T's Negligence in Safeguarding Plaintiff's and Class Members' Private Information

45. AT&T was bound by contractual obligations, industry standards, common law principles, and representations made to the Plaintiff and Class Members. These obligations mandated the confidentiality of their Private Information and the implementation of measures to prevent unauthorized access and disclosure.

46. Plaintiff and Class Members entrusted their Private Information to AT&T with a

¹² FN 1, *supra*.

¹³ *Id.*

¹⁴ Troy Hunt, *Inside the Massive Alleged AT&T Data Breach*, TroyHunt.com (Mar. 19, 2024), <https://www.troyhunt.com/inside-the-massive-alleged-att-data-breach/> (last visited on Apr. 9, 2024).

¹⁵ *Id.*

¹⁶ *Id.*

reasonable expectation and mutual understanding that AT&T would fulfill its obligations to maintain the confidentiality and security of such information, safeguarding it from unauthorized access.

47. AT&T's data security obligations were especially critical given the significant rise in cyberattacks and data breaches leading up to the breach date.

48. Considering recent high-profile data breaches at other companies, AT&T was aware or should have been aware that electronic records would become prime targets for cybercriminals.

49. Accordingly, cyberattacks have gained such notoriety that both the Federal Bureau of Investigation and the U.S. Secret Service have issued warnings to potential targets, urging them to be vigilant and prepared for potential attacks. As one report elucidated, "[e]ntities such as smaller municipalities and hospitals are appealing to ransomware criminals . . . because they often possess weaker IT defenses and a strong incentive to swiftly regain access to their data."¹⁷

50. Hence, the surge in such attacks, along with the associated risk of future incidents, was common knowledge among the public and within AT&T's industry, including AT&T itself.

51. AT&T failed to implement adequate data security measures to safeguard Plaintiff's and Class Members' Private Information as evidenced by the database stolen by ShinyHunters in 2021 and by the full leak of about 73 million individuals' Private Information by MajorNelson in 2024, nearly three years after the 2021 Data Incident.

52. Despite the initial Data Incident occurring in August 2021 (and recurring in March 2024), AT&T has taken no action to inform the public about the gravity of the Data Breach. Furthermore, AT&T has failed to provide potential victims of the Data Breach with guidance on how to safeguard their Private Information.

¹⁷ *FBI, Secret Service Warn of Targeted*, Law360 (Nov. 18, 2019), <https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware> (last visited Apr. 9, 2024).

53. Despite the compromise and leakage of Private Information persisting for approximately two and a half years, AT&T has taken no action to remove the leaked Private Information from unauthorized locations, such as internet forums, which are accessible on the Clear Web.

54. Additionally, AT&T has taken no steps to ascertain the source of the Data Breach. This is apparent from AT&T's hesitancy to confirm whether the Data Breach could be traced back to a third-party partner entrusted with processing and safeguarding a significant portion of the Plaintiff's and Class Members' Private Information.

55. Given that the Data Breach stemmed from malicious actors like ShinyHunter and MajorNelson exploiting a data security vulnerability within one of AT&T's third-party processors of Private Information, AT&T neglected to sufficiently verify the effectiveness of security measures, if any, implemented by such third-party processors to safeguard the Private Information.

D. AT&T's Non-Compliance with FTC Guidelines

56. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

57. In 2016, the FTC revised its publication, "Protecting Personal Information: A Guide for Business," which outlined cybersecurity guidelines for businesses. These guidelines emphasize that businesses should prioritize the protection of personal customer information they retain, appropriately dispose of unnecessary personal information, encrypt data stored on computer networks, comprehend their network vulnerabilities, and establish policies to rectify any security issues.¹⁸ The guidelines also

¹⁸ *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Apr. 9, 2024).

recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.¹⁹

58. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

59. The FTC has brought enforcement actions against businesses for failing to protect customer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

60. AT&T neglected to adequately adopt fundamental data security measures. By failing to utilize reasonable and appropriate safeguards against unauthorized access to Private Information, AT&T engaged in an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

61. AT&T was at all times fully aware of its responsibility to safeguard the Private Information of its customers. Moreover, AT&T was well aware of the substantial repercussions that would ensue from its failure to fulfill this obligation.

E. AT&T’s Non-Compliance to Industry Standards

62. As illustrated earlier, cybersecurity experts frequently emphasize companies’

¹⁹ *Id.*

heightened vulnerability to cyberattacks because of the substantial value associated with the PII they collect and maintain.

63. Accordingly, numerous best practices have been identified, which companies like AT&T should, at a minimum, adopt. These include, but are not limited to, ensuring that Private Information is only shared with third parties when reasonably necessary and that those vendors have adequate cybersecurity systems and protocols in place.

64. Numerous industry and national best practices have been published and should serve as primary resources when establishing an institution's cybersecurity standards. For instance, the Center for Internet Security (CIS) introduced its Critical Security Controls (CSC), which all businesses are strongly encouraged to adhere to. The CIS Benchmarks are widely preferred by auditors globally for guiding organizations in adopting a secure build standard for various governance and security initiatives, including PCI DSS, NIST 800-53, SOX, FISMA, ISO/IEC 27002, Graham Leach Bliley, and ITIL.²⁰

65. Additional standard cybersecurity practices in the telecommunications industry encompass installing suitable malware detection software; monitoring and restricting network ports; securing web browsers and email management systems; configuring network systems such as firewalls, switches, and routers; monitoring and safeguarding physical security systems; fortifying against potential communication system vulnerabilities; and providing comprehensive staff training on critical security protocols.

F. Heightened Risk of Fraud and Identity Theft Due to Cyberattacks and Data Breaches

66. In a 2007 report on data breaches ("GAO Report"), the United States Government

²⁰ See *CIS Benchmarks FAQ*, Center for Internet Security, <https://www.cisecurity.org/cis-benchmarks/cis-benchmarks-faq/> (last visited Apr. 9, 2024).

Accountability Office highlighted that victims of identity theft would encounter "significant costs and time to rectify the harm to their reputation and credit history."²¹

67. Any victim of a data *breach* faces significant repercussions, regardless of the type of data compromised. Cybercriminals target personally identifiable information with the aim of profiting from it. They achieve this by selling the acquired data on the black market to identity thieves, who exploit it to extort, harass, and assume victims' identities for unlawful financial activities. As a person's identity resembles a puzzle, the more accurate pieces of data obtained by identity thieves, the simpler it becomes for them to assume the victim's identity or engage in harassment or surveillance.

68. The FTC advises identity theft victims to undertake several measures to safeguard their personal and financial information following a data breach. These steps include contacting one of the credit bureaus to place a fraud alert—considering an extended fraud alert lasting for 7 years if their identity is stolen—reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and rectifying any inaccuracies in their credit reports.²²

69. Identity thieves exploit pilfered personal information, such as Social Security numbers, to perpetrate an array of crimes, including but not limited to credit card fraud, phone or utilities fraud, and bank/finance fraud.

70. Identity thieves have various nefarious ways of exploiting Social Security numbers.

²¹ See U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (2007). Available at <https://www.gao.gov/new.items/d07737.pdf> (last visited Apr. 9, 2024).

²² See *IdentityTheft.gov*, Federal Trade Commission, <https://www.identitytheft.gov/Steps> (last visited Apr. 9, 2024).

They can procure a driver's license or official identification card in the victim's name but with the thief's photograph. Additionally, they might use the victim's name and Social Security number to unlawfully acquire government benefits or file a fraudulent tax return. Moreover, these perpetrators could secure employment using the victim's Social Security number, rent a property in the victim's name, and potentially provide the victim's personal information to law enforcement during an arrest, leading to the issuance of an arrest warrant under the victim's name.

71. Moreover, theft of Private Information is also gravely serious. PII is a valuable property right.²³

72. Its value is self-evident, particularly in light of the significance of "big data" in corporate America and the substantial penalties associated with cyber thefts. Even a cursory risk-to-reward analysis underscores the undeniable market value of Private Information.

73. Notably, there may be a significant time gap, often measured in years, between when harm occurs and when it is detected, as well as between the theft of Private Information and its subsequent use.

74. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at p. 29.

²³ *See, e.g.,* John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

75. Private Information holds such immense value for identity thieves that once compromised, criminals frequently trade it on the "cyber black market" for years on end.

76. There is a high likelihood that entire sets of stolen information have already been dumped on the black market, and more batches may follow suit. This indicates that Plaintiff and Class Members face an elevated risk of fraud and identity theft for many years to come.

77. Therefore, Plaintiff and Class Members must diligently monitor their financial accounts and other associated accounts for an extended period.

78. Sensitive Private Information can be sold for as much as \$363 per record, as reported by the Infosec Institute.²⁴ PII holds significant value because criminals can exploit it to target victims with various frauds and scams. Once PII is compromised, the fraudulent use of that information and subsequent harm to victims may persist for years.

79. For instance, the Social Security Administration has cautioned that identity thieves can exploit an individual's Social Security number to apply for additional credit lines. Such fraudulent activities may remain unnoticed until debt collection calls begin months or even years later. Additionally, stolen Social Security Numbers enable thieves to file fraudulent tax returns, claim unemployment benefits, or even secure employment using a false identity. Detecting each of these fraudulent activities is challenging. Individuals may remain unaware that their Social Security Number was used for unemployment benefits until law enforcement notifies their employer of suspected fraud. Similarly, fraudulent tax returns are usually detected only when an individual's genuine tax return is rejected.

80. Furthermore, changing or canceling a stolen Social Security number is a daunting task.

²⁴ See Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), <https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/>.

An individual cannot acquire a new Social Security number without extensive paperwork and evidence of actual misuse. Moreover, even with a new Social Security number, its effectiveness is questionable. As noted, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."²⁵

81. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."²⁶

82. Due to the immense value of the data it collects and stores, the telecommunications industry has witnessed a disproportionately higher frequency of data theft incidents compared to other sectors.

83. Consequently, AT&T was well aware or should have been cognizant of these risks and should have fortified its data protocols accordingly. Despite being alerted to the significant and predictable risk of harm from a data breach, AT&T neglected to adequately ready itself for such an eventuality.

G. Plaintiff's and Class Members' Damages

84. To date, AT&T has taken no action whatsoever to redress the grievances endured by the Plaintiff and other Class Members due to the Data Breach.

85. The compromise of their Private Information in the Data Breach has caused tangible

²⁵ Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft>.

²⁶ Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), <http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html>.

harm to the Plaintiff and other Class Members.

86. On March 7, 2024, Plaintiff Cameron King, an 18-year customer of AT&T, received an email from AT&T that his Private Information was involved in the Data Breach.

87. Further investigation by Plaintiff King revealed that the Data Breach encompassed the Private Information of 73 million AT&T customers.

88. Subsequent verification by the Plaintiff has established that his Private Information was unequivocally affected by the Data Breach. Furthermore, it has come to light that his Private Information can be readily accessed through a search of the publicly available database containing AT&T customers' Private Information.

89. Plaintiff's Private Information was compromised as a direct and proximate result of the Data Breach.

90. As a direct and proximate result of AT&T's conduct, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

91. As a result of the Data Breach, the Private Information of over 73 million AT&T customers, including Plaintiff King and Class Members, are available on the Internet for users, including criminals, to find, search through, and download.

92. Due to the direct and proximate consequences of AT&T's actions, the Plaintiff and Class Members have been compelled to allocate significant time towards addressing the ramifications of the Data Breach.

93. The Plaintiff and Class Members are confronted with a significant risk of incurring out-of-pocket fraud losses, including but not limited to loans initiated in their names, unauthorized medical services billed to them, tax return fraud, utility accounts fraudulently opened in their names,

credit card misuse, and other forms of identity theft.

94. Plaintiff and Class Members are exposed to a significant risk of becoming targets for future phishing attempts, data intrusions, and other illicit schemes, leveraging their Private Information. The potential exists for fraudsters to exploit this information to orchestrate such schemes more efficiently, directly putting the Plaintiff and Class Members at heightened risk.

95. The Plaintiff and Class Members may also face financial burdens associated with protective measures, including expenses for credit monitoring services, credit report fees, costs associated with implementing credit freezes, and other related expenses directly or indirectly stemming from the Data Breach.

96. Plaintiff and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

97. Plaintiff and Class Members suffered additional harm through benefit-of-the-bargain damages. They paid for a service with the expectation of adequate data security, but this was not fulfilled. Part of the remuneration provided to AT&T was intended to ensure the robust security of the Plaintiff's and Class Members' Private Information. Consequently, they did not receive the level of protection they rightfully paid for.

98. Plaintiff and Class Members have devoted, and will continue to devote, considerable time to overseeing their financial accounts and records for any signs of misuse. Notably, AT&T has failed to furnish any guidance to the Plaintiff and Class Members regarding the extensive time they must dedicate to monitoring their accounts, nor have they received instructions on how to implement a security freeze on their credit reports.

99. Plaintiff and Class Members have endured or will endure actual harm directly

stemming from the Data Breach. Many victims have incurred quantifiable losses, including: (a) Detecting fraudulent charges; (b) Cancelling and reissuing credit and debit cards; (c) Acquiring credit monitoring and identity theft prevention services; (d) Addressing their inability to access funds associated with compromised accounts; (e) Making trips to banks and enduring waiting times to access funds from restricted accounts; (f) Implementing freezes and alerts with credit reporting agencies; (g) Spending time communicating with financial institutions or visiting them in person to dispute fraudulent charges; (h) Reaching out to financial institutions to close or alter financial accounts; (i) Reconfiguring automatic billing and payment instructions from compromised cards to new ones; (j) Incurring late fees and declined payment charges resulting from failed automatic payments linked to cancelled compromised cards; (k) Vigilantly scrutinizing and monitoring Social Security Numbers, medical insurance accounts, bank accounts, and credit reports for unauthorized activity in the foreseeable future.

100. Furthermore, the Plaintiff and Class Members have a vested interest in safeguarding their Private Information, which is believed to still be within the possession of AT&T, to prevent further breaches. This entails the implementation of robust security protocols and safeguards, such as ensuring that data or documents containing personal and financial information are not accessible online, employing password protection for access to such data, and ensuring that all sensitive data is adequately encrypted.

101. Further, as a result of AT&T's conduct, Plaintiff and Class Members are forced to live with the anxiety that their Private Information—which contains the most intimate details about a person's life—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

102. Due to the direct consequences of the AT&T's actions and inactions, the Plaintiff and

Class Members have experienced a significant loss of privacy and are now confronted with an imminent and heightened risk of future harm.

CLASS ALLEGATIONS

103. Plaintiff brings this Action as a class action under Federal Rule of Civil Procedure 23 and seeks certification of the following nationwide Class:

All individuals residing in the United States whose personal information was accessed, compromised, copied, stolen, and/or disclosed due to the data breach involving AT&T, Inc. (The “Class”).

104. Excluded from the Class are AT&T, its officers and directors, and Members of their immediate families or their legal representatives, heirs, successors or assigns and any entity in which AT&T has or had a controlling interest.

105. Class certification of Plaintiff's claims is appropriate because Plaintiff can prove the elements of the claims on a class-wide basis utilizing the same evidence as would be used to prove those elements in separate actions alleging the same claims.

106. **Numerosity**—Federal Rule of Civil Procedure 23(a)(1). The Members of the Class are so numerous that joinder of all Class Members would be impracticable. Upon information and belief, the Class number is over 70 million. Also, the Class is comprised of an easily ascertainable set of AT&T customers who were impacted by the Data Breach. The exact number of Class Members can be confirmed through discovery, which includes AT&T's records. The resolution of Plaintiff's and Class Members' claims through a class action will behoove the Parties and this Court.

107. **Commonality and Predominance**—Federal Rule of Civil Procedure 23(a) (2) and 23(b)(3). Common questions of fact and law exist as to all Members of the Class and predominate over questions affecting only individual Class Members. These common questions of law or fact, include, among other things:

- a. Whether AT&T's cybersecurity systems and/or protocols complied with relevant data security laws and industry standards before and during the Data Breach;
- b. Whether AT&T effectively implemented purported security measures to safeguard Plaintiff's and Class Members' Private Information from unauthorized access, dissemination, and misuse;
- c. Whether AT&T took reasonable steps to ascertain the extent of the Data Breach upon discovery;
- d. Whether AT&T disclosed Plaintiff's and Class Members' Private Information contrary to the understanding that it would be kept confidential;
- e. Whether AT&T willfully, recklessly, or negligently failed to maintain and enforce reasonable procedures and security controls to prevent unauthorized access to Plaintiff's and Class Members' Private Information;
- f. Whether AT&T was unjustly enriched by its actions; and
- g. Whether Plaintiff and Class Members are entitled to damages, injunctive relief, or other equitable relief, and the extent thereof.

108. AT&T engaged in a common course of conduct granting rise to the legal rights sought to be enforced by Plaintiff, on behalf of himself and other Members of the Class. Similar or identical common law violations, business practices, and injuries are involved.

109. **Typicality**—Federal Rule of Civil Procedure 23(a)(3). Plaintiff's claims are typical of the claims of the other Members of the Class because, *inter alia*, all Class Members were similarly injured and sustained similar monetary and economic injuries as a result of AT&T's misconduct described herein and were accordingly subject to the alleged Data Breach. Also, there are no defenses available to AT&T that are unique to Plaintiff.

110. **Adequacy**—Federal Rule of Civil Procedure 23(a)(4). Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the Class he seeks to represent, he retained counsel competent and experienced in complex class action litigation, and he will prosecute this action earnestly. The Class’s interests will be fairly and adequately protected by Plaintiff and his counsel.

111. **Injunctive Relief**—Federal Rule of Civil Procedure 23(b)(2). AT&T acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate regarding the Class under Federal Rule of Civil Procedure 23(b)(2).

112. **Superiority**—Federal Rule of Civil Procedure 23(b)(3). A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiff and the other Class Members are relatively small compared to the burden and expense that would be required to litigate their claims on an individual basis against AT&T, making it impracticable for Class Members to individually seek redress for AT&T’s wrongful conduct. Even if Class Members could afford individual litigation, the court system could not. Individualized litigation would create a potential for inconsistent or contradictory judgments and increase the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

113. Class certification is also warranted under Rules 23(b)(1) and/or (b)(2) because:

- a. Prosecuting separate actions by individual Class Members could lead to inconsistent or varying adjudications, establishing conflicting standards of

conduct for AT&T;

- b. Pursuing separate actions by individual Class Members may result in adjudications that could be decisive for the interests of other Class Members not involved in the adjudications, or could significantly hinder or obstruct their ability to safeguard their interests; and
- c. AT&T's actions and refusals to act are generally applicable to the Class, thereby necessitating appropriate final injunctive relief concerning the Class Members collectively.

114. Class certification is further justified as this Court has the authority to allocate specific claims or issues for class-wide treatment and may establish multiple subclasses under Federal Rule of Civil Procedure 23(c)(4).

CAUSES OF ACTION

COUNT I NEGLIGENCE

(On Behalf of Plaintiff and the Class)

115. Plaintiff repeats and re-alleges each and every factual allegation contained in paragraphs 1-114 as if fully set forth herein. Plaintiff brings this claim individually and on behalf of the Class.

116. In order to access telecommunications services, AT&T mandated that Plaintiff and Class Members provide non-public Private Information, including PII.

117. Plaintiff and Class Members entrusted their Private Information to AT&T with the expectation that AT&T would diligently safeguard their information.

118. By collecting and retaining this data within its computer systems, and by sharing and exploiting it for commercial purposes, AT&T had a duty of care to employ reasonable measures to

secure and protect its computer assets —along with the Private Information of Class Members stored within them—to avert information disclosure and prevent theft. AT&T's obligation encompassed thoroughly assessing vendors with whom it exchanged Private Information, ensuring these vendors maintained adequate data security protocols and procedures.

119. AT&T owed a nondelegable duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

120. AT&T owed a nondelegable duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information's duty of care to use reasonable security measures arose as a result of the special relationship that existed between AT&T owed a nondelegable duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information and its customers, which is recognized by laws and regulations, as well as common law.

121. AT&T was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

122. AT&T owed a nondelegable duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information had a duty to employ reasonable security measures under Section 5 of the Federal

Trade Commission Act, 15 U.S.C. § 45, which prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

123. AT&T owed a nondelegable duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information’s duty to use reasonable care in protecting confidential data arose not only as a result of the law described above, but also because AT&T is bound by industry standards to protect confidential Private Information.

124. AT&T breached its duties, and thus was negligent, by failing to use reasonable measures in its own systems to protect Class Members’ Private Information and by failing to properly verify that its third-party processors implemented data security measures adequate to safeguard Plaintiff’s and Class Member’s Private Information.

125. It was foreseeable that AT&T’s failure to use reasonable measures to protect Class Members’ Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the telecommunications industry.

126. It was therefore foreseeable that the failure to adequately safeguard Class Members’ Private Information would result in one or more types of injuries to Class Members.

127. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

128. Plaintiff and Class Members are further entitled to injunctive relief mandating that AT&T: (i) enhance its data security protocols and procedures; (ii) undergo future annual audits of said

systems and monitoring procedures; and (iii) continue providing sufficient credit and identity monitoring services to all Class Members.

COUNT II

NEGLIGENCE *PER SE* (On Behalf of Plaintiff and the Class)

129. Plaintiff repeats and re-alleges each and every factual allegation contained in paragraphs 1-128 as if fully set forth herein. Plaintiff brings this claim individually and on behalf of the Class Members.

130. Plaintiff and Class Members are within the class of persons that the FTCA was intended to protect.

131. The harm stemming from the Data Breach aligns with the type of harm the FTCA was designed to prevent. The FTC has taken enforcement actions against businesses that, due to their failure to implement reasonable data security measures and avoid unfair and deceptive practices, inflicted similar harm to that experienced by Plaintiff and the Class.

132. AT&T breached its duties and obligations by neglecting to implement industry-standard data and cybersecurity measures to ensure compliance with applicable laws.

133. It was reasonably foreseeable, particularly given the growing number of data breaches of personal information in the telecommunications sector, that the failure to reasonably protect and secure Plaintiff's and Class Members' Private Information in compliance with applicable laws would result in an unauthorized third-party gaining access to Plaintiff's and Class Members' Private Information.

134. The Private Information of Plaintiff and Class Members, constitutes personal property, was pilfered as a consequence of AT&T's negligence, leading to harm, injury, and damages for Plaintiff and Class Members.

135. AT&T's actions directly led to the unauthorized access and disclosure of Plaintiff's and Class Members' unencrypted Private Information, resulting in ongoing damages for Plaintiff and Class Members. They seek damages and other forms of relief due to AT&T's negligence.

COUNT III

BREACH OF IMPLIED CONTRACT (On Behalf of Plaintiff and the Class)

136. Plaintiff repeats and re-alleges each and every factual allegation contained in paragraphs 1-135 as if fully set forth herein. Plaintiff brings this claim individually and on behalf of the Class Members.

137. Through their interactions and course of conduct, AT&T, Plaintiff, and Class Members implicitly entered into contracts for the provision of telecommunications services, along with implicit agreements for AT&T to establish sufficient data security measures to safeguard and preserve the privacy of Plaintiff's and Class Members' Private Information.

138. Specifically, Plaintiff entered into a valid and enforceable implied contract with AT&T when he signed up with AT&T for telecommunications services.

139. The valid and enforceable implied contracts for telecommunications services, entered into by Plaintiff and Class Members with AT&T, inherently entail the commitment to safeguard non-public Private Information entrusted to AT&T or generated by AT&T itself, preventing its disclosure.

140. Therefore, when Plaintiff and Class Members supplied their Private Information to AT&T in exchange for telecommunications services, they implicitly entered into contracts with AT&T, whereby AT&T undertook the obligation to reasonably safeguard such information.

141. AT&T solicited and invited Class Members to provide their Private Information as part of AT&T's regular business practices. Plaintiff and Class Members accepted AT&T's offers and provided their Private Information to AT&T.

142. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that AT&T's data security practices complied with relevant laws and regulations and were consistent with industry standards.

143. Plaintiff and Class Members who paid money to AT&T reasonably believed and expected that AT&T would allocate part of those funds to ensure adequate data security. AT&T failed to do so.

144. Under the implied contracts, AT&T promised and was obligated to: (a) provide telecommunications services to Plaintiff and Class Members; and (b) protect Plaintiff's and the Class Members' Private Information. In exchange, Plaintiff and Members of the Class agreed to pay money for these services and to provide their Private Information.

145. Both the provision of telecommunication services and the protection of Plaintiff's and Class Members' Private Information were material aspects of these implied contracts.

146. The implied contracts for the provision of telecommunications services, encompassing the contractual obligations to uphold the privacy of Plaintiff's and Class Members' Private Information, are acknowledged, memorialized, and embodied in multiple documents, including AT&T's Privacy Notice.

147. AT&T's express representations, including those explicitly outlined in its Privacy Notice but not limited to it, serve to memorialize and embody the implied contractual obligation mandating AT&T to implement data security sufficient to safeguard and protect the privacy of Plaintiff's and Class Members' Private Information.

148. Customers of telecommunications services highly value their privacy, as well as that of their dependents, and prioritize the confidentiality of their PII in connection with procuring such services. For individuals like Plaintiff and Class Members, telecommunications services lacking

adherence to industry-standard data security protocols for safeguarding Private Information are inherently less valuable and less desirable compared to those that do adhere to such standards. Plaintiff and Class Members would not have entrusted their Private Information to AT&T nor entered into these implied contracts without the understanding that their Private Information would be safeguarded and protected. It was implicit in their engagement with AT&T that reasonable data security measures would be adopted.

149. Plaintiff and Class Members fulfilled their contractual obligations by remitting payment for their telecommunications services and furnishing their Private Information as required.

150. AT&T materially breached its contractual duty to safeguard the non-public Private Information it had collected when unauthorized individuals gained access to this sensitive data during the cyberattacks and Data Breach.

151. AT&T materially violated the terms of the implied contracts, as outlined in the pertinent Privacy Notice, by failing to uphold the privacy of Plaintiff's and Class Members' Private Information. This breach is evident through the repeated unauthorized disclosures of Private Information to at least two cybercriminal actors—ShinyHunters and MajorNelson. AT&T's actions fell short of industry standards and the standards of conduct outlined in statutes like Section 5 of the FTCA, thereby failing to adequately protect Plaintiff's and the Class Members' Private Information, as detailed above.

152. The Data Breach was a reasonably foreseeable consequence of AT&T's actions in breach of these contracts.

153. Due to AT&T's breach of the promised data security protections, Plaintiff and Class Members did not receive the full benefit of the telecommunications services as described in the contracts. As a result, they suffered damages equivalent to the disparity between the value of the

telecommunications services with the promised data security and the services actually received.

154. Had AT&T disclosed that it did not adhere to industry-standard security measures, neither the Plaintiff, the Class Members, nor any reasonable person would have purchased telecommunications services from AT&T.

155. As a direct and proximate result of the Data Breach, Plaintiff and Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation the release and disclosure of their Private Information, the loss of control of their Private Information, the imminent risk of suffering additional damages in the future, disruption of their telecommunications services, out-of-pocket expenses, and the loss of the benefit of the bargain they had struck with AT&T.

156. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

157. Plaintiff and Class Members are entitled to injunctive relief, including, but not limited to, requiring AT&T to: (i) enhance its data security systems and monitoring procedures; (ii) undergo annual audits of said systems and procedures; (iii) ensure the adequacy of security measures implemented by third-party processors of AT&T's Private Information; and (iv) offer sufficient credit and identity monitoring to all Class Members.

COUNT IV

UNJUST ENRICHMENT (On Behalf of Plaintiff and the Class)

158. Plaintiff repeats and re-alleges each and every factual allegation contained in paragraphs 1-157 as if fully set forth herein. Plaintiff brings this claim individually and on behalf of the Class Members.

159. The Plaintiff and Class Members conferred a monetary benefit upon AT&T by

engaging in transactions for the acquisition of goods and services, thereby furnishing their Private Information to AT&T. It was expected that in return for this exchange, the Plaintiff and Class Members would receive the goods and services outlined in the transaction, alongside the assurance that their Private Information would be safeguarded through sufficient data security measures.

160. AT&T knew that Plaintiff and Class Members conferred a benefit which AT&T accepted. AT&T profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes.

161. The funds paid by the Plaintiff and other Class Members for goods and services were allocated, in part, to cover the expenses associated with utilizing AT&T's network, as well as the administrative costs related to data management and security.

162. In accordance with principles of equity and good conscience, it is imperative that AT&T not be allowed to retain the funds rightfully belonging to the Plaintiff and the Class Members because the AT&T neglected to implement the necessary data management and security measures as required by industry standards.

163. AT&T's failure to secure the private information of the Plaintiff and the Class Members resulted in inadequate compensation for the value they provided.

164. AT&T obtained the Private Information through unfair and inequitable means, as it failed to disclose the previously alleged inadequate security practices.

165. Had the Plaintiff and the Class Members been aware that AT&T had not adequately secured their Private Information, they would not have consented to use AT&T's services.

166. Plaintiff and Class Members have no adequate remedy at law.

167. As a direct and proximate result of the AT&T's conduct, the Plaintiff and Class Members have suffered and will suffer injury, including but not limited to (a) actual identity theft, (b)

loss of control over Private Information usage, (c) compromise and theft of Private Information, (d) out-of-pocket expenses for prevention and recovery, (e) lost productivity, (f) ongoing risk due to inadequate security, and (g) future costs for addressing the impact of the Data Breach.

168. As a direct and proximate result of AT&T's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

169. AT&T should be compelled to disgorge proceeds unjustly received from the Plaintiff and Class Members into a common fund or constructive trust, for their benefit. Alternatively, the AT&T should refund the amounts overpaid by the Plaintiff and Class Members for AT&T's services.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the Class seek the following relief:

- a. an order certifying this action as a Class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and confirming Plaintiff as a suitable representative of the Nationwide Class sought herein;
- b. judgment in favor of Plaintiff and Class Members, granting them suitable monetary relief, comprising actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;
- c. an order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;
- d. an order instructing AT&T to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members;
- e. an order requiring AT&T to pay the costs involved in notifying Class Members about the judgment and administering the claims process;

- f. judgment in favor of Plaintiff and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and
- g. an award of such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury of all triable claims.

Dated: April 9, 2024

Respectfully submitted,

/s/ Joe Kendall

JOE KENDALL

Texas Bar No. 11260700

KENDALL LAW GROUP, PLLC

3811 Turtle Creek Blvd., Suite 825

Dallas, Texas 75219

Telephone: 214/744-3000 / 214/744-3015 (fax)

jkendall@kendalllawgroup.com

Sabita J Soneji (*pro hac vice forthcoming*)

TYCKO AND ZAVAREEI LLP

1970 Broadway

Suite 1070

Oakland, CA 94612

510-254-6808

Email: ssoneji@tzlegal.com

Attorneys for Plaintiff and the Proposed Class